WHAT IS CLAIMED IS:

1. In a network node, a method for performing cryptographic-related functions, comprising:

receiving an input requiring cryptographic-related processing;

generating a message based on the input, the message representing one of a predefined set of messages for processing by a cryptographic processing component;

transmitting the message to the cryptographic processing component; and

performing the cryptographic-related processing.

2. The method of claim 1, wherein the cryptographic-related processing includes at least one of:

verifying or generating a digital signature; encrypting data; decrypting data; retrieving a digital certificate or certificate revocation list; verifying a certificate's hierarchy; self-signed certificate processing; retrieving, verifying and storing a digital certificate in the node; and certificate age checking.

3. The method of claim 1, wherein the node includes at least one application program, the method further comprising:

executing the input via the application program; and

wherein the generating a message includes:

generating the message via the application program.

4. The method of claim 1, wherein the node includes at least one application program, the method further comprising:

generating an output message via the application program, the output message requiring cryptographic-related processing;

transmitting, based on the required cryptographic-related processing, one of the predefined set of messages to the cryptographic processing component;

performing the cryptographic-related processing; and

outputting the processed message.

5. A computer-readable medium having stored thereon a plurality of sequences of instructions that may be invoked by a plurality of predefined messages, said instructions including sequences of instructions which, when executed by a processor, cause said processor to perform the steps of:

receiving an input representing one of the predefined messages;

transmitting, based on the input, a request for cryptographic-related processing to a cryptographic processing module; and

performing the cryptographic-related processing.

6. The computer-readable medium of claim 5, wherein the performing the cryptographic-related processing includes at least one of:

verifying or generating a digital signature; encrypting or decrypting data; retrieving a digital certificate or certificate revocation list; verifying a certificate's

hierarchy; self-signed certificate processing; retrieving, verifying and storing a digital certificate; and certificate age checking.

7. The computer-readable medium of claim 5, wherein the transmitting includes:

sending a function call to the cryptographic processing module.

8. The computer-readable medium of claim 5, wherein the input represents a digitally signed network control message requiring verification.

9. A cryptographic module, comprising:

a memory configured to store a plurality of cryptographic processing programs, each program being invoked via one of a plurality of predefined messages; and

a processor configured to:

receive an input requiring cryptographic-related processing,

generate one of the predefined messages based on the input,

transmit the message to a first one of the cryptographic processing programs, and

perform the cryptographic-related processing.

10. The cryptographic module of claim 9, wherein when performing the cryptographic-related processing, the processor is configured to perform at least one of:

verifying or generating a digital signature; encrypting data; decrypting data; retrieving a digital certificate or certificate revocation list; verifying a certificate's hierarchy; self-signed certificate processing; retrieving, verifying and storing a digital certificate; and certificate age checking.

11. The cryptographic module of claim 9, wherein when transmitting the message, the processor is further configured to:

transmit a function call to the first cryptographic processing program.

12. The cryptographic module of claim 9, wherein the processor is further configured to:

transmit the result of the cryptographic-related processing to an application program.

13. A cryptographic module, comprising:

means for storing a plurality of cryptographic processing programs, each program being invoked via one of a plurality of predefined messages;

means for receiving an input requiring cryptographic-related processing;

means for generating one of the predefined messages based on the input;

means for transmitting the message to a first one of the cryptographic processing programs; and

means for performing the cryptographic-related processing.

14. In a node coupled to other nodes in a network, the node including an application program for handling communications with the other nodes, a method of performing cryptographic-related functions, the method comprising:

receiving an input requiring a cryptographic-related operation;

generating a predefined message based on the input, the message representing one of a plurality of predefined messages usable by a cryptographic processing program;

transmitting the predefined message to the cryptographic processing program; and

performing, via the cryptographic processing program, the desired cryptographic-related operation.

15. The method of claim 14, further comprising:

returning the result of the performing to the application program.

16. The method of claim 14, wherein the predefined message includes at least one of:

a request for digital signature generation, a request for digital signature verification, a request for data encryption, a request for data decryption, a request for retrieval of a digital certificate, a request for retrieval of a certificate revocation list, a request for verification of a certificate's hierarchy, a request for self-signed certificate processing, and a request for certificate age checking.

17. The method of claim 16, wherein the request for digital signature generation includes a request for at least one of RSA signature generation, secret keyed MD5 signature generation, elliptic curve signature generation and digital signature standard signature generation.

18. The method of claim 16, wherein the request for digital signature verification includes a request for at least one of RSA signature verification, secret keyed MD5 signature verification, elliptic curve signature verification and digital signature standard signature verification.

19. The method of claim 16, wherein the request for data encryption includes a request for at least one of RSA based encryption and elliptic curve based encryption.

20. The method of claim 16, wherein the request for data decryption includes a request for at least one of RSA based decryption and elliptic curve based decryption.

21. The method of claim 14, wherein the performing includes:

accessing a remote server via the network to retrieve cryptographic-related information.

22. A computer-readable medium that stores instructions executable by at least one processor to perform a method for providing cryptographic-related functions, comprising:

receiving a first function call from a predefined list of function calls, the predefined list of function calls representing available cryptographic-related functions executable by the at least one processor;

generating a request message based on the first function call, the request message representing a request for processing by a cryptographic processing module;

transmitting the request message to the cryptographic processing module; and

performing the cryptographic-related function.

23. A system for performing cryptographic-related functions, comprising:

a call handler component configured to receive a function call from an application program and generate a request message;

a request handler configured to receive the request message and generate a corresponding instruction request; and

a cryptographic processing component configured to receive the instruction request and perform cryptographic-related processing.